SV

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/864,110	05/24/2001	William Alton Fiveash	AUS9-2000-0924-US1	1467

40412 7590 08/17/2005

IBM CORPORATION- AUSTIN (JVL)
C/O VAN LEEUWEN & VAN LEEUWEN
PO BOX 90609
AUSTIN, TX 78709-0609

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 08/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/864,110	FIVEASH ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/14/05 3/28/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 6/3/2005.

Response to Arguments

The rejection of claims 1-20 under 35 USC 112 2nd Paragraph has been withdrawn due to the amendments to the independent claims 1, 8, and 14, which have corrected the clarity issue.

Applicant's arguments with respect to claim 6/3/2005 have been considered but are moot in view of the new ground(s) of rejection.

Furthermore, the examiner would like to note the statement made by the applicant in the last paragraph of page 9 through the first paragraph of page 10 in the communication dated 6/3/2005. The applicant states that because Elgamal fails to mention certificate revocation, it could not be possible for it to be obvious to use certificate revocation in Elgamal. The examiner disagrees with this statement entirely. The examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, as shown below, simply because Elgamal did not specifically address certificate revocation, does not mean it would not be obvious to use certificate revocation in combination with Elgamal.

Claims 1-21 have been examined.

All objections and rejections not set forth below have been withdrawn.

Information Disclosure Statement

The information disclosure statements (IDS) submitted on 3/14/2005 and 3/28/2005 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 7-12, 14-18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal et al. (US Patent Number 5,657,390) hereinafter referred to as Elgamal, and further in view of Housley et al (RFC 2459) hereinafter referred to Housley.

Regarding claim 1, Elgamal disclosed a method of establishing a secure communication path between two computer systems (See Elgamal Col. 3 Paragraph 3) comprising: creating a communication path to exchange data, (See Elgamal Col. 6 Line 57 – Col. 7 Line 12) including identification data and digital certification data, between the two systems (See Elgamal Fig. 4 and Col. 7 Lines 13-40 and Fig. 5 and Col. 8 Line 45 – Col. 10 Line 23); determining, based on the identification data, whether to confirm the digital certification data (See Elgamal Figs. 4-5, Col. 7 Lines 20-65, Col. 10 Lines 3-23, Col. 20 Lines 25-32, Col. 22 Line 56 – Col. 23 Line18); and creating a secure communication path, without confirming the digital certification data if it is

determined the digital certification data should not be confirmed (See Elgamal Fig. 5 and corresponding text) , or after confirming the digital certification data if it is determined that the digital certification data should be confirmed (See Elgamal Fig. 4 and Corresponding text), but failed to disclose that confirming the digital certification data included verifying that the certificate had not been revoked. However, Elgamal did disclose that the certificates used in the system were X.509 certificates (See Elgamal Col. 30 Lines 14-19).

Housley teaches that when verifying an X.509 certificate, a certificate revocation list should be checked in order to ensure that the certificate has not become invalid (See Housley Page 12 Section 3.3).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Housley in the certificate verification of Elgamal by verifying that the certificate was not on a certificate revocation list when verifying the certificates. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that invalidated certificates were not being trusted.

Regarding claim 8, Elgamal disclosed an information handling system comprising: one or more processors; a memory accessible by the processors; a nonvolatile storage accessible by the processors; a network interface connecting the information handling system to a computer network (See Elgamal Col. 3 Lines 46-55); and a network security tool to create a secure path between computer systems (See Elgamal Col. 3 Paragraph 3), the network security tool including: means for creating a communication path to exchange data, (See Elgamal Col. 6 Line 57 – Col. 7 Line 12) including identification data and digital certification data, between the two systems (See Elgamal Fig. 4 and Col. 7 Lines 13-40 and Fig. 5 and Col. 8 Line 45 – Col. 10 Line

23); means for determining, based on the identification data, whether to confirm the digital certification data (See Elgamal Figs. 4-5, Col. 7 Lines 20-65, Col. 10 Lines 3-23, Col. 20 Lines 25-32, Col. 22 Line 56 – Col. 23 Line18); and means for creating a secure communication path, without confirming the digital certification data if it is determined the digital certification data should not be confirmed (See Elgamal Fig. 5 and corresponding text) , or after confirming the digital certification data if it is determined that the digital certification data should be confirmed (See Elgamal Fig. 4 and Corresponding text), but failed to disclose that confirming the digital certification data included verifying that the certificate had not been revoked. However, Elgamal did disclose that the certificates used in the system were X.509 certificates (See Elgamal Col. 30 Lines 14-19).

Housley teaches that when verifying an X.509 certificate, a certificate revocation list should be checked in order to ensure that the certificate has not become invalid (See Housley Page 12 Section 3.3).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Housley in the certificate verification of Elgamal by verifying that the certificate was not on a certificate revocation list when verifying the certificates. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that invalidated certificates were not being trusted.

Regarding claim 14 Elgamal disclosed a computer program product stored on a computer operable medium for providing one or more secure connections form a computer system (See Elgamal Abstract and Claims), said computer program product comprising: means for creating a communication path to exchange data, (See Elgamal Col. 6 Line 57 – Col. 7 Line 12) including

identification data and digital certification data, between the two systems (See Elgamal Fig. 4 and Col. 7 Lines 13-40 and Fig. 5 and Col. 8 Line 45 – Col. 10 Line 23); means for determining, based on the identification data, whether to confirm the digital certification data (See Elgamal Figs. 4-5, Col. 7 Lines 20-65, Col. 10 Lines 3-23, Col. 20 Lines 25-32, Col. 22 Line 56 – Col. 23 Line18); and means for creating a secure communication path, without confirming the digital certification data if it is determined the digital certification data should not be confirmed (See Elgamal Fig. 5 and corresponding text) , or after confirming the digital certification data if it is determined that the digital certification data should be confirmed (See Elgamal Fig. 4 and Corresponding text), but failed to disclose that confirming the digital certification data included verifying that the certificate had not been revoked. However, Elgamal did disclose that the certificates used in the system were X.509 certificates (See Elgamal Col. 30 Lines 14-19).

Housley teaches that when verifying an X.509 certificate, a certificate revocation list should be checked in order to ensure that the certificate has not become invalid (See Housley Page 12 Section 3.3).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Housley in the certificate verification of Elgamal by verifying that the certificate was not on a certificate revocation list when verifying the certificates. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that invalidated certificates were not being trusted.

Regarding claim 21, Elgamal disclosed a method of establishing a secure communication path between two computer systems comprising (See Elgamal Col. 3 Paragraph 3): creating a communication path to exchange data, including identification data and digital certification data,

between the two systems (See Elgamal Col. 6 Line 57 – Col. 7 Line 12 and Fig. 4 and Col. 7 Lines 13-40 and Fig. 5 and Col. 8 Line 45 – Col. 10 Line 23), determining, based on the identification data, whether to confirm the digital certification data (See Elgamal Figs. 4-5, Col. 7 Lines 20-65, Col. 10 Lines 3-23, Col. 20 Lines 25-32, Col. 22 Line 56 – Col. 23 Line18), wherein the determining includes consulting an internal table, the internal table including identification data of all computer systems for which it is not necessary to confirm the certification data (See Elgamal Col. 10 Lines 3-23); creating a secure communication path, without confirming the digital certification data if it is determined the digital certification data should not be confirmed (See Elgamal Fig. 5 and corresponding text) , or after confirming the digital certification data if it is determined that the digital certification data should be confirmed (See Elgamal Fig. 4 and Corresponding text); selecting a local-remote pair from an endpoints table corresponding to the computer systems (See Elgamal Col. 9 Line 59 - Col. 10 Line 6); selecting a policy from a policy table based on the selected local-remote pair, the policy including one or more access methods (See Elgamal Col. 9 Line 59 - Col. 10 Line 6); and transmitting one or more security proposals corresponding to the selected policy to the remote computer system (See Elgamal Col. 10 Lines 3-6), but failed to disclose that confirming the digital certification data included verifying that the certificate had not been revoked. However, Elgamal did disclose that the certificates used in the system were X.509 certificates (See Elgamal Col. 30 Lines 14-19).

Housley teaches that when verifying an X.509 certificate, a certificate revocation list should be checked in order to ensure that the certificate has not become invalid (See Housley Page 12 Section 3.3).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Housley in the certificate verification of Elgamal by verifying that the certificate was not on a certificate revocation list when verifying the certificates. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that invalidated certificates were not being trusted.

Regarding claims 2, 9, and 15, the combination of Elgamal and Housley disclosed that the determining step includes the step of consulting an internal table, the internal table including identification data of all computer systems for which it is not necessary to confirm that digital certification data has not been revoked (See Elgamal Col. 8 Lines 45-61 and Col. 10 Lines 3-23 and Housley Page 12 Section 3.3).

Regarding claims 3, 10, and 16, the combination of Elgamal and Housley disclosed he two computer systems include a local and a remote computer system, the exchanged data further including one or more authentication proposals from the local computer system and a selected authentication proposal from the remote system (See Elgamal Col. 5 Paragraph 3 and Col. 10 Lines 3-23).

Regarding claims 4, 11, and 17, the combination of Elgamal and Housley disclosed selecting an access method in response to determining to confirm whether the digital certification data has not been revoked; and invoking the selected access method (See Elgamal Col. 7 Lines 13-40 and Housley Page 12 Section 3.3).

Regarding claims 5, 12, and 18, the combination of Elgamal and Housley disclosed selecting a local-remote pair from an endpoints table corresponding to the computer systems (See Elgamal Col. 8 Line 45 – Col. 9 Line 31); selecting a policy from a policy table based on

the selected local-remote pair, the policy including one or more access methods (See Elgamal Col. 9 Lines 9-14); and transmitting one or more security proposals corresponding to the selected policy to the remote computer system (See Elgamal Col. 10 Lines 3-6).

Regarding claims 7 and 20, the combination of Elgamal and Housley disclosed digitally signing a message using a private key corresponding to one of the computer systems; and sending the signed message to the other computer system (See Elgamal Figs. 4 and 5 and Col. 8 Lines 5-20).

Claims 6, 13, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Elgamal and Housley as applied to claims 1, 8, and 14 above, and further in view of Schneier (Applied Cryptography).

Elgamal and Housley disclosed receiving a remote digital certificate from the other computer system (See Elgamal Col. 7 Lines 20-26), but Elgamal failed to disclose verifying the certification authority signature on the certificate. However, Elgamal did disclose issuing a "bad certificate" error if the signature on the certificate was bad (See Elgamal Col. 20 Lines 25-33).

Schneier teaches that certification authorities sign certificates, and that in order to verify whether a certificate is bad or not, the signature of the certification authority on the certificate must be verified (See Schneier Pages 185 – 186 Section Entitled "Public-key Certificates", Especially page 186 Lines 1-8).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the certificate authentication of Elgamal and Housley by checking to make sure the signature on the certificate was the signature of a trusted certification authority. This would have been obvious because the ordinary person skilled in the

art would have been motivated to ensure that the public key in the certificate was the public key of the remote party in order to protect against substitution man-in-the-middle attacks.

Conclusion

Claims 1-21 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Rivest ("Can We Eliminate Certification Revocation Lists") disclosed a method in which a certificate is checked on revocation lists only if a specified date is expired in the certificate.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Patent Examiner
Art Unit 2131
8/8/2005

Primary Examiner
AU 2131
8/15/05